PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G07F 7/10

A1

(11) International Publication Number: **WO 99/64996**

(43) International Publication Date: 16 December 1999 (16.12.99)

(21) International Application Number: PCT/IB99/00977

(22) International Filing Date: 1 June 1999 (01.06.99)

(30) Priority Data:
98110350.0 5 June 1998 (05.06.98) EP

(71) Applicant *(for all designated States except US)*: LANDIS & GYR COMMUNICATIONS S.A.R.L. [CH/CH]; 70, rue du Grand-Pré, CH-1211 Geneva 2 (CH).

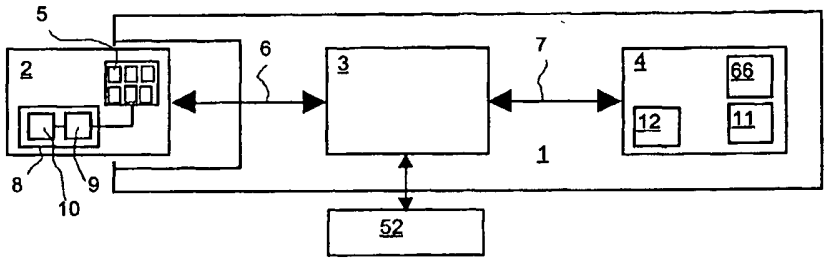
(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: CAMBOIS, Etienne [FR/FR]; 5, lotissement Plein Soleil, F-26110 Montmeyran (FR).

(74) Agent: WENGER, Joël; Griffes Consulting S.A., 81, route de Florissant, CH-1206 Geneva (CH).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: PRELOADED IC-CARD AND METHOD FOR AUTHENTICATING THE SAME



(57) Abstract

A system comprising a card reader (1) with a terminal (3) and a security module (4) accepts a portable preloaded IC-card (2) having an integrated circuit (8) with a lock (9) to prevent unauthorised use of the IC-card (2), and a cash value unit counter content (10), which represents the cash value and is devaluated during a transaction at a stand alone point of sale. The IC-card (2) generates a card random number, whereas the security module (4) generates a security module random number. The IC-card (2) encodes the security module random number into a card signature, and the security module (4) decodes the card signature again to verify the authenticity of the IC-card (2). The security module (4) creates a security module signature from the card random number being decoded by the IC-card (2) to verify the authenticity of the security module (4). If the mutual authentication is positive, the lock (9) allows the payment transaction to take place.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

PRELOADED IC-CARD AND METHOD FOR AUTHENTICATING THE SAME

The invention relates to preloaded IC-cards and a system for mutual authentications between preloaded IC-cards and card readers and a method for the mutual authentications according to the generic part of claims 1, 4 and 10.

Such preloaded IC-cards and systems for authentication of preloaded IC-cards and of associated card readers are to be used in mobile or public telephones, commodity metering devices, vending machines, point of sales and the like.

IC-cards are based on the DE-PS 25 60 080 and DE-PS 25 12 935 and are used world wide, today. The exchange of information between a card reader and the IC-card may be blocked for writing into sections of a memory already occupied by data.

The application WO97/21197 describes the payment operation with preloaded IC-cards of prior art identifying the IC-card prior to the payment operation and checking thereafter the correct devaluation of the IC-card content.

The US-A 4'710'613 teaches to use an identification system to check the validity of the data transfer between a card reader and the IC-card. After inserting the IC-card into the card reader the user inputs a personal identification number to the card reader generating in turn an identification code information using the RSA encryption algorithm and calculates an estimation of the time required for processing the identification code information by a processor of the IC-card. The card reader measures the actual time required for processing the identification code information by the IC-card processor and blocks any further data transfer, if the actual processing time does not meet the estimated time.

The WO9424673 presents an IC-card containing a microprocessor and non-volatile memory sections divided into pages. The microprocessor writes only into one page at a time. The memory allocates a first region of a non-volatile memory for data and a second region of non-volatile memory for status information. A data write operation is performed by writing data to the first region and writing information to a second region, if the data write operation was performed successfully. This procedure confirms and signifies a fully completed data transfer.

The US-A 5'572'004 describes a method of payment for services or goods using the preloaded IC-card which communicates with a security module through an electronic

terminal located in the card reader. The method ensures the correct devaluation of the IC-card and the correct amount transferred from the IC-card to the security module of the card reader.

From the FR-A 2 580 834 is known to protect the memory against fraudulent inspection with a shield. The shield comprises resistive layers over the integrated circuit representing two of the four resistors of the Wheatstone's bridge integrated into the integrated circuit. Any physical damage to the shield will be sensed by the integrated circuit and the integrated circuit will disable any further access.

These IC-cards having cryptographic abilities are used as electronic purses. Before any transaction takes place, the owner of the purse or smart card has to identify himself to the card reader terminal by a personal identification number. The card reader presents a signature based on the personal identification number to the IC-card which in turn is checked by the IC-card, if the personal identification number is valid or not. The signature is also called a "Cryptogram". In case of a valid personal identification number, the card reader is allowed to proceed with the transaction, e.g. to read the monetary value of the IC-card and to change the monetary value of the IC-card by a certain amount in order to pay for the transaction.

In contrast the preloaded IC-card may be used like money, any bearer of the IC-card is authorised to use it without identification. An authentication of the IC-card is made by the card reader terminal in conjunction with a security module. As the number of card readers is growing, it will be impossible to keep track on the exact location of obsolete card readers with still functioning security modules. A fraudulently altered card reader may deplete the IC-card of its total amount of cash value instead of the exact amount signalled to the owner of the card at the point of sale and illegally transfer the money worth to the security module of the altered card reader. Later the cash value stored in the security module will be unsuspiciously transferred to the bank account of the trickster.

Most of the IC-cards are standardised according to ISO/IEC 7816, parts 1 to 5.

The primary objects of the present invention are to prevent unauthorised cash value transfer between a IC-card and a not identified card reader and its security module, respectively, and to provide a system comprising the card reader and the preloaded

IC-card connected to the card reader, and a method for this system which is secure, and the IC-card.

These objects will be met according to the present invention by the characterising features of Claims 1, 6 and 10.

A complete understanding of the present invention will be accomplished by reading the detailed description of a preferred embodiment thereof in conjunction with the drawings,

wherein

Figure 1 is schematic view of a system for mutual authentication of preloaded IC-cards,

Figure 2 is a block diagram of an integrated circuit of the IC-card,

Figure 3 is a flowchart of a mutual authentication operation,

Figure 4 is a flowchart of a payment transaction

Figure 5 shows a random number generator circuit,

Figure 6 shows a counter record,

Figure 7 shows a backup counter area,

Figure 8 is a flowchart of a key change operation,

Figure 9 shows a brute force attack counter,

Figure 10 shows two memory sections and

Figure 11 visualises an integrity check.

In figure 1 identifies 1 a card reader, 2 an IC-card, 3 an electronic terminal of the card reader 1, 4 a security module, 5 contact pads, 6 data lines, 7 a socket for the security module 4, 8 an integrated circuit, 9 an electronic lock, 10 a cash value unit counter content, 11 a T-DES unit to produce a security module signature, and 12 a random number generator. The electronic circuit 8 is implemented as a tiny module into a flat piece of plastic representing the IC-card 2. The contact pads 5 of this module enables the electronic circuit 8 to communicate with the terminal 3. The card reader 1 is part of or connected to a stand alone point of sale 52, e.g. a payphone, a low value point of sale, a commodity metering device, a vending machine and the like, and operate

without direct connection to an external host computer in contrast to devices for smart cards. Besides the mechanical parts which are not shown here, the card reader 1 provides a bay or a slot to accommodate one IC-card 2, and comprises further the electronic terminal 3 controlling the read-/write operation in conjunction with the security module 4. At least one security module 4 (ETSI EN726-7) used in the card reader 1 has a standardised size looking like a small IC-card 2 (CEN/ENV 1375 - "Additional ICC Formats, - part 1: ID-000 Card"), and is able to verify the IC-cards 2 of one Issuer and to handle the transactions of the identified IC-cards 2. If the IC-card 2 is inserted into the card reader 1, the contact pads 5 are brought into contact with contact fingers (not shown here) of the card reader 1, so that the terminal 3 is able to exchange data with the IC-card 2 by means of the data lines 6. Each security module 4 is inserted into the socket 7 to connect it to the terminal 3 for easy exchange or removal, and provides the terminal 3 with specific data of the IC-card 2 for security purposes and memory spaces for the amount of the cash value units collected from the IC-card 2. The socket 7 and the data line 6 are indicated in the drawing by double headed arrows indicating the data traffic directions to and from the terminal 3. All data to be exchanged between the IC-card 2 and the security module 4 are handled by the terminal 3. The card reader 1 represents the outside world for the IC-card 2.

Other executions of the system use electromagnetic waves to establish a bi-directional data link between the terminal 3 and the IC-card 2. The IC-card 2 may have these electromagnetic contact means in combination with the data transfer across the contact pads 5 and the card reader 1 will activate the appropriate contact means.

As in prior art, the integrated circuit 8 of the preloaded IC-card 2 stores a card identification number and the cash value unit content counter 10 in its memory which is protected by the electronic lock 9. The security module 4 identifies the IC-card 2 by its identification number and, if the test is positive, the lock 9 is opened and the cash value units are transferred from the IC-card 2 to the security module 4. The drawbacks of this system have been mentioned in the introductory part. Therefore the preloaded IC-card 2 has additional features so that the security module 4 not only identifies the IC-card 2 but also vice versa, i.e. the IC-card 2 is able to check the authenticity of the security module 4 in use.

Figure 2 shows the IC-card 2 and in more details the integrated circuit 8 which allows such a mutual authentication between the security module 4 (figure 1) and the IC-card 2. The integrated circuit 8 may be a microprocessor based on an 8-bit micro controller 13. Memory sections 14 to 20, and a physical security unit as the lock 9, and a dedicated asynchronous receiver/transmitter unit 21 are connected to this controller 13 by a 12 bit wide address bus 22 and a bi-directional 8 bit wide data bus 23. A reset line 24 allows to reset the controller 13 and the lock 9 by the terminal 3 (figure 1). Just for the record, the lock 9 and the receiver/transmitter unit 21 are connected directly to the controller 13 by interrupt and status lines. The terminal 3 sends by means of the contact pads 5 synchronised to a clock signal on a clock line 25 the data to be transferred over a bi-directional single wire input/output - line 26 to the integrated circuit 8 or receives the data from the integrated circuit 8. The asynchronous receiver/transmitter unit 21 serves as an interface to the data bus 22 controlled by the controller 13. The contact pads 5 allow further a connection of the reset line 24, the clock line 25, and the power supply lines (not shown here) to the terminal 3. The data transmission over the single wire input/output line 26 may be standardised according the ISO/IEC standard 7816-3 (1989): electronic signal and transmission protocols, including amendment 1 (1992): clause 9 and is characterised as asynchronous half duplex block transmission according to protocol T=1.

The memory may be divided into seven memory sections 14 to 20 storing data and program information. A read only memory (= ROM) is provided for the sections 14 and 15. The two ROM sections 14 and 15 may be of a flash memory type or a conventional ROM, having together e.g. 4096 bytes. The third section 16 is a random access memory (RAM memory section 16) with a capacity of e.g. 128 bytes which may provide a RAM area 49 for data to be lost due to a reset or a power cut-off. The remaining memory cells having e.g. 176 bytes are of the electrically erasable and programmable ROM (=E^2PROM) cells type and are divided into the four sections 17 to 20. The E^2PROM memory sections 17 to 20 provide the non volatile storage space for sensitive or secret data, e.g. for a secret cryptographic key K in the third memory section 19, for the cash value unit counter content 10 in the forth E^2PROM memory section 20, for a life cycle status LS in the first E^2PROM memory section 17, etc. and are protected against analysing, e.g. by use of a scanning electron microscope, by a special shield 27 covering these E^2PROM memory sections 17 to 20. The physical

integrity of the shield 27 is at least tested by the controller 13 during each power-up step (figure 3) of the IC-card 2. Any physical damage to the shield 27 will be sensed and causes the controller 13 to set the life cycle status LS to "Not Valid" and to erase the content of all cells in the E^2PROM memory sections 17 to 20 where confidential data are stored, e.g. by resetting all these cells of the E^2PROM memory sections 17 to 20 to zero, and the secret data are lost. At least the cryptographic key K has to be erased to render the IC-card 2 useless.

The lock 9 comprises a generator circuit 28 for generating a card random number, an electronic circuitry as an algorithm unit 29 which is e.g. made of hardwired logic elements for executing a DES transformation and capable of a very fast computing (in the order of a millisecond) of a card signature according to the TRIPLE DATA ENCRYPTION STANDARD (= T-DES: DES and T-DES, see "Applied Cryptography" by Bruce Schneier, ISBN 0-471-11709-9, p. 294). The DES transformation and the inverse DES transformation are used for encoding and decoding according to the T-DES transformation and are handled by the same algorithm unit 29 and by the T-DES unit 11 (figure 1), respectively. The cryptographic key K is used in the T-DES coding procedure for sensitive data to be exchanged between the IC-card 2 and the security module 4. Therefore the IC-card 2 and the security module 4, both store in their respective memories the identical cryptographic key K and use the identical algorithm in the algorithm unit 29 and in the encoder 11 (figure 1), respectively, to encode and decode the data exchanged. Another task of lock 9 is to decode any access request by the terminal 3 to the IC-card 2, to compare the request with the life cycle status LS (e.g. "Test Mode", "Issuer Mode", "User Mode", "Not Valid"), and act accordingly. The life cycle test starts each time, the IC-card 2 is connected to the power supply of the card reader 1 (figure 1). The lock 9 reads the life cycle status LS. The "Test Mode" is only used once for factory quality control using a test program located in the first ROM 14 which disables itself after the "Test Mode" - program has been executed. The second ROM 15 stores an operating program. The controller 13 runs under the operating program if the life cycle status LS of the IC-card 2 is in "Issuer Mode" or "User Mode" and will be activated by the test program. In the "Issuer Mode", also used only once, at least an individual card number, the cash value unit counter contents 10 (figure 1), the date, the keys, other necessary parameters of the IC-card 2, etc. are fed to the E^2PROM memory sections 17 to 20 under control of the

operating program. If the IC-card 2 is issued to the user, the lock 9 has normally to distinguish only between "Not valid" and the "User Mode". In the "User Mode" a check is made on the stored number of invalid access attempts. If the limit of the invalid access attempts has been surpassed, the life cycle status LS is set to "Not Valid". There is no possibility to reset the life cycle status LS = "Not Valid". If the lock 9 does not detect the life cycle status LS = "User Mode" a signal on an invalidate line 30 blocks any access to the memory section 14 to 20. A faulty access number 48 located e.g. in the fourth E^2PROM memory section 20 limits the unsuccessful access attempts to a certain limit. In the "Issuer Mode" the number of maximum allowed unsuccessful access attempts is stored as the faulty access number 48. To transfer status information out of the IC-card 2 a life cycle status byte may be used which is stored in the RAM memory section 16. For example seven bits of the life cycle status in the first E^2PROM memory section 17 are copied into the life cycle status byte. The eighth bit represents an authenticate flag indicating the status of the present authentication process. The following procedures are explained on the assumption that in the "Issuer Mode" the faulty access number 48 is set to a number, e.g. to 15 or "F" in hexadecimal notation.

Figure 3 shows a schematic flowchart of the mutual authentication process between the IC-card 2 and the card reader 1 (figure 1). The flow chart indicates which steps occur in the IC-card 2, the terminal 3, and the security module 4, respectively. The mutual authentication process begins at power - up step 31 after the terminal 3 contacts the IC-card 2 and supplies the electrical power. A reset signal on the reset line 24 (figure 2) is sent to the IC-card 2 during a reset step 32. The controller 13 (figure 2) is set to a start address and overwrites in turn the RAM memory section 16 (figure 2). The reset signal initialises the lock 9 (figure 2), too, in order to start a life cycle test on the life cycle status LS during a preparation step 33. Using a comparator 47 (figure 2) of the lock 9 the controller 13 compares the faulty access number 48 with zero at a card check 331. If the faulty access number 48 equals zero, no more authentications are allowed and the IC-card 2 will be invalidated during an invalidate step 332 by setting the life cycle status LS to "Not Valid" and after erasing the confidential data, and the process is send to an out step 333. Otherwise, the process continues with a random number step 334. The life cycle status LS is now in the "User Mode", and the generator circuit 28 (figure 2) prepares a card random number

and the controller 13 stores the card random number at the RAM area 49 of the RAM memory section 16 and proceeds to the out step 333, too. There, the life cycle status byte is refreshed and is transferred together with relevant data, if any to the terminal 3. The relevant data are e.g. the individual card serial number, an integrated circuit number, the date of issue, the number of cash value units, the card random number, etc. After having received at least the refreshed life cycle status byte the terminal 3 tests the actual life cycle status byte during a terminal check 34 and, if the IC-card 2 is in the "User Mode", the terminal 3 initialises the authentication in a initialisation step 35 by sending the relevant data of the IC-card 2 and a initialisation request to the security module 4; otherwise if the life cycle status byte is set to "Not Valid" the process is terminated by the terminal 3 at stop 36. In the generator step 37 the random number generator 12 (figure 1) generates a security module random number which is stored in the security module 4 together with the relevant data of the IC-card 2, The security module random number is send back to the terminal 3 at a receiving step 38. Then the terminal 3 forwards the security module random number as a encoding request 39 to the lock 9 and initialises a card encoding step 40 starting with a decrement of the faulty access number 48 by one unit. Then the algorithm unit 29 (figure 2) calculates a card signature which is the T-DES - transformation of the security module random number and the relevant data of the IC-card 2 using the cryptographic key K. The card signature and the security module random number are stored at the RAM area 49, too. The card signature is sent back to the terminal 3 together with the refreshed life cycle status byte. The terminal 3 sends the card signature as an authentication request 41 to the security module 4, where during the authentication test 42 the T-DES unit 11 (figure 1) decodes the transferred card signature with the cryptographic key K, e.g. by comparing the transferred card signature with the card signature recalculated by the T-DES unit 11 using the cryptographic key K and the stored original security module random number and the relevant data of the IC-card 2 stored in the security module 4. According to the result of the comparison a security module status byte is set to "Card Authentic" if the IC-card 2 is acceptable or - if not - to "Card Not Authentic". If the security module status byte is "Card Authentic", the card signature is stored in the security module 4 and the T-DES unit 11 using the cryptographic key K encodes a security module signature based on the card random number and the previous result of the authentication, i.e.

the card signature. The security module signature, if any, and the security module status byte are presented to the terminal 3. If a decision 43 establishes the security module status byte to be "Card Not Authentic" the process is aborted at a stop 44. However, if the card signature is correct and the IC-card 2 therefore acceptable to the security module 4, the decision 43 based on the security module status byte branches the process to a verifying request 45. There the terminal 3 presents the security module signature to the lock 9. During the verifying step 46 the lock 9 tests the security module signature. The algorithm unit 29 (figure 2) recalculates the security module signature with the cryptographic key K and the card signature stored in the RAM memory section 16 and the original card random number, and the controller 13 compares the result with the transmitted security module signature using the comparator 47. If the recalculated and the transmitted security module signatures are equal, the mutual authentication is valid, the faulty access number 48 is incremented by one unit, and the authenticate flag is set to "Access OK". However, if the recalculated and the transmitted security module signatures are different, the authentication failed and the authenticate flag is set to "Access Not OK. The IC-card 2 sends the refreshed life cycle status byte to the terminal 3 which tests the life cycle status byte again in a second decision 50. If the life cycle status byte indicates the "User Mode" and the authenticate flag signals that the security module 4 is acceptable for the IC-card 2 ("Access OK"), the lock 9 is unlocked and allows the cash value unit counter content 10 (figure 2) in the fourth memory section 20 to be changed. The mutual authentication is successfully ended at service step 51 and the terminal 3 in connection with the authorised security module 4 is allowed to proceed with a payment transaction. If the second decision 50 senses a faulty authentication, i.e. the authenticate flag is set to "Access Not OK", the process ends at the stop 44. At the end of the successful mutual authentication process both devices, the IC-card 2 and the security module 4, have stored in the respective memories the card signature and the security module signature.

The figure 4 represents a schematic flowchart of a payment transaction procedure in which authentication is rechecked before the cash value is transferred from the IC-card 2 to the security module 4. After the mutual authentication has been correctly processed and the terminal 3 has reached the service step 51, the terminal 3 accepts from the point of sale 52 a payment request 53 with a transaction value, i.e. the

number of the cash value unit to be decreased in the cash value unit counter content 10 (figure 2). Only if the transaction value is less than the cash value unit counter content 10, the terminal 3 proceeds with the procedure and sends a decrease request 54 and the transaction value to the security module 4. Based on the previously calculated and stored security module signature and the transaction value a new security module signature is established in a signature step 55 and replaces the previous security module signature in the memory. At a reception step 56 the terminal 3 receives the new security module signature and presents it together with the transaction value in a requesting step 57 to the lock 9 (figure 2) of the IC-card 2. In an arithmetic step 58 the controller 13 decrements firstly the faulty access number 48 by one unit and sets the authenticate flag to "Access Not OK". Then the algorithm circuit 29 (figure 2) recalculates the new security module signature in the arithmetic step 58 based on the old security module signature stored at the RAM area 49 in the RAM memory section 16 (figure 2) and the transaction value. The old security module signature is replaced by the new security module signature at RAM area 49. If the result of this calculation is the same as the transferred new security module signature, the authentication is verified. The actual cash value unit counter content 10 is copied as a previous cash value unit counter content 10' into the fourth E^2PROM memory section 20 and is thereafter decreased by the transaction value to get a present cash value unit counter content 10, i.e. the present cash value is the difference of the previous cash value minus the transaction value. After the decrease of the cash value unit counter content 10 is completed, the controller 13 (figure 2) increments the faulty access number 48 (figure 2) by one unit and sets the authenticate flag to "Access OK". The refreshed life cycle status byte is sent to the terminal 3 where a third decision 59 on this status byte branches the procedure. If the authenticate flag indicates "Access Not OK", the terminal 3 aborts the procedure at stop 60. If the third decision 59 senses the authenticate flag in the status "Access OK", the terminal 3 sends a signature request 61 to the IC -card 2. In a coding step 62 IC-card 2 generates a new card signature in the algorithm circuit 29 based on the cryptographic key K, the present cash value and the previously used card signature. The new card signature replaces the old card signature in the RAM memory section 16 and is sent to the terminal 3 (terminal step 63). In the meantime, the security module 4 has calculated separately the present cash value from the data stored in

the security module 4 in order to enhance security and to save transmission time on the input/output line 26 (figure 2). The terminal 3 transfers in a transfer step 64 the new card signature to the security module 4 and initialises an incrementing step 65 wherein the new card signature replaces the stored old one. The T-DES unit 11 (figure 1) verifies based on the previously used card signature and the present cash value the authenticity of the new card signature. If the authenticity of the new card signature is true, the status byte is set to "OK" and a transaction counter 66 (figure 1) is incremented by the transaction value, if the authenticity is not verified only the security module status byte is set to "Not OK". The security module status byte is returned to the terminal 3 to be tested in a fourth decision 67. If the security module status byte is "Not OK" then the transaction procedure is terminated at stop 68. However, if the security module status byte is "OK" then the terminal 3 has finished the transaction procedure successfully and the payment will be acknowledged to the point of sale 52 in an acknowledge step 69. Then the terminal 3 returns to the service step 51 awaiting a new transaction procedure or the removal of the IC-card 2. From the terminal step 63 onwards the transaction procedure runs independently of any connection to the IC-card 2, up to the acknowledge step 69 and from there to the service step 51 or, if the IC-card 2 is removed, the terminal 3 goes asleep until the next contact with an IC-card 2 will occur.

If a process ends at the stops 36 (figure 3), 44 (figure 3) and 60, the IC-card 2 is locked by the signal on the invalidate line 30 (figure 3) and has to be reset by a signal on the reset line 24 (figure 2) at the reset step 32 (figure 3), in order to restart the authentication process again. An other execution of the terminal 3 restarts automatically the authentication process and/or the transaction procedure a limited number of times at the stops 44 and/or 60 by returning to the reset step 32.

The surveillance of the mutual authentication process covers at least the preparation and exchange periods of the encrypted data, i.e. from the start of the encoding step 40 (figure 3) to the second decision 50 (figure 3) and during the arithmetic step 58, and has the advantage to recognise any access ending irregularly, e.g. due to a non valid IC-card 2, a power failure or a disconnecting of the IC-card 2 from the card reader 1 (figure 1) and to limit the number of these irregular accesses by decrementing the faulty access number 48 stored in the E^2PROM memory section 20. The preparation and exchange periods of the encrypted data involve time

consuming calculations and may last up to several seconds and therefore sufficient time is available to end the mutual authentication processes in an irregular way.

The transaction procedure has the advantage that the data flow on the single wire input/output line 26 is drastically reduced and the calculation time in the respective circuits of the IC-card 2 and of the security module 4 is minimised without sacrificing security. The cryptographic processes save advantageously time by calculating only two random numbers at the very beginning of the authentication process and using thereafter the previous respective signatures instead of the time consuming generation and exchange of new random numbers.

The life cycle status LS may be set by the terminal 3 under certain conditions the terminal 3 contacts the IC-card 2 actively, e.g. at the reset step 32 (figure 3), at the encoding request 39 (figure 3), at the verifying request 45 (figure 3), at the request step 57, at the signature request 61, etc. As an example, such a condition may arise in case the security module 4 detected that the transferred card number is listed as stolen or otherwise suspicious. In case the life cycle status LS is set to "Not Valid", the controller 13 erases at least the confidential cryptographic keys in the third E^2PROM memory section 19 as described above.

In figure 5 a generator device 70 is shown which may be used as the random number generator 12 (figure 1) and the generator 28 (figure 2) for generating the security module random number and the card random number, respectively. The device 70 comprises a linear shift register 71, a free-running clock 72, and Boolean units 73. In the example shown the shift register 71 of eight bits is shifting its content from the least significant bit to the most significant bit, e.g. in the drawing of figure 5 the shift register 71 is shifting its content to the right. The outputs of actual contents of the most significant or eighth bit and of the sixth bit and of the third bit are mixed together by the Boolean units 73 with a signal of the free-running clock 72 to form a combined signal fed to the input of the least significant bit. The signal of the free-running clock 72 is asynchronous to the clock signal of the shift register 71. The kind of the Boolean units 73 and the signals of the shift register 71 to be combined by the Boolean units 73, the size of the shift register 71 and the frequency of the free-running clock 72 are determined by the requirements for the generator device 70, e.g. the random numbers produced by the device 70 must be compliant to basic statistical distribution

laws and the criteria developed by S. W. Golomb ("Shift Register Sequences" by S. W. Golomb, Holden-Day, San Fancisco 1967 or second edition at Aegean Park Press, 1982).

Returning now to figure 2. The feature of tracking of the number of invalid access attempts and limiting this number to a predetermined number of allowed invalid access attempts has the advantage that the cryptographic key K for the signature generation used by the algorithm circuit 29 cannot be extracted by trial and error attack, hence the cryptographic key K is kept secret. The decrease of the faulty access number 48 prior to the authentication process prevents the fooling of the system by tearing the IC-card 2 from the card reader 1 (figure 1) before the faulty access number 48 is incremented again at the end of the successful transaction at the verifying step 46 and the arithmetic step 58 (figure 4).

In another execution of the IC-card 2 the authentication test is started at the beginning of the preparation step 33 instead of the encoding step 40 (figure 3) in order to keep the whole procedure from the preparation step 33 until the end of the verifying step 46 under surveillance.

In another execution of the IC-card 2 the controller 13 is programmed to compare a set of two numbers directly under control of the operating program which eliminates the need of the hardwired comparator 47.

The cash value unit counter content 10 is stored in the fourth memory section 20 and the cash value units are decremented by the controller 13 as demanded by the terminal 3 until all the cash value units are used up and the cash value is zero. Then the IC-card 2 is used up and discarded.

An execution of the IC-card 2 is able to be reloaded to a predetermined cash value limit, e.g. the equivalent of CHF 300.00. At one of its E^2PROM memory sections 17 to 20 a number of allowed reloads is stored which is set in the "Issuer mode". If the number of allowed reloads is set to zero, the IC-card 2 can be used once, up to the moment the cash value unit counter content 10 reaches zero. As long as the number of allowed reloads is different to zero, the terminal 3 (figure 1) may request the IC-card 2 to get ready to reload the cash value unit counter content 10. This service may be initialised after the mutual authentication has been established at the service step 51 (figure 3). The controller 13 tests the number of allowed reloads. If the number of

allowed reloads is not zero, then the controller 13 decrements the number of allowed reloads by one unit and the cash value unit counter content 10 can accept new cash value units. The reload will take place at a specialised card reader 1 connected to a computer of a bank institute instead to the point of sale 52 (figure 1). Besides the mutual authentication between the IC-card 2 and the card reader 1, an additional identification of the user by means of the personal identification number is required by the bank institute. The number of reloads will be advantageously limited in order to minimise any misuse and to invalidate IC-cards 2 of high age to avoid misfunction due to the limited lifetime of the E^2PROM memory cells.

The limits for e.g. the cash value unit counter content 10, the faulty access number 48, the number of reloadings etc., are set in the "Issuer mode" to the maximum allowed numbers which are stored in the memory section 20. The appropriate limit will be decreased at least by one unit, if a respective event has occurred. This method has the advantage of time saving because the controller 13 compares the respective numbers much faster with zero than it executes a comparison with a number stored in the memory. At the verification step 46 and the arithmetic step 58 the faulty access number 48 may be incremented by one unit.

The system of the preloaded IC-card 2 and the card reader 1 (figure 1) has the advantage that the preloaded IC-card 2 and the security module 4 (figure 1) are able to mutually authenticate the partner of the data transfer and provides the system with means to refuse any non - authentic access attempt to the user's payment means. This enhances greatly the level of confidence a customer can put into his IC-card 2 and the Issuer into the whole system.

To enhance the integrity of the memory of the IC-card 2, the integrated circuit 8 has to prevent effects due to sudden power failures, e.g. in case the IC-card 2 is torn away from the card reader 1 (figure 1) before the transaction has finished or during an updating of one of the counting areas in the E^2PROM memory sections 17 to 20. In prior art of preloaded card technology a hard wired logic prevents the effects of card withdrawal during the updating of the counting area by using a flag or witness bit which is written each time the counter content 10 is changed. Since it is impossible to write the witness bit exactly in parallel with the counter, there is still a possibility that

error may occur due to a sudden power failure. This may even result in a state where the counter content 10 can be illegally increased.

The new IC-card 2 is provided with automatic backup means for each sensitive counter to keep track of the counter content changes by storing at least the previous and the actual content of the respective counters.

In figure 6 a counter record 74 is shown as an example. The counter record 74 comprises three fields, a management field 75 indicating the seniority of the counter record 74, a counter value 76 storing the actual IC-card value 10 (figure 2) at the time the counter record 74 was saved, and a checksum in a checksum field 77, the content of which (the checksum) is based on the counter value 76. Each sensitive counter of the IC-card 2 has at least two counter records 74 located in a backup counter area 78 of the memory section 20. The integer number of the counter records 74 is greater than 1, but less than the capacity of the management field 75. The most sensitive counter deals with the cash value units. The further description refers to the cash value unit counter.

In the example shown in figure 7, the backup counter area 78 has a set of four counter records 74. The controller 13 determined during the preparation step 33 (figure 3) a maximal value of the contents in the four management fields 75a to 75d of the backup counter area 78, and stored said maximum value of the four management fields 75a to 75d into an activation field 79 located in the RAM memory section 16. The controller 13 will always overwrite the oldest entry in the backup counter area 78. The address of the oldest entry is calculated according to the rule: "the content of the activation field 79 increased by one and taken as modulo the number of counter records 74a to 74d in the backup counter area 78".

If the counter content, i.e. the. cash value unit counter content 10 (figure 2), has to be changed, the controller 13 gets access over the data bus 23 to the memory section 20 with the backup counter area 78. Then the controller 13 reads out the content of the activation field 79 and determines the address of one of the counter record 74a to 74d by the operation "content of the activation field 79 modulo 4", e.g. counter record 74b, which has been used at the previous change of the counter and recalculates the checksum based on the counter value 76b, e.g. the cash value unit counter content 10. If the recalculated checksum is the same as the checksum stored in field 77b then

the previous change of the counter was successfully terminated. The controller 13 increments the content of the activation field 79 by one unit, reads out the counter value 76b, and reduces the content of the counter value 76b by a decrement of one or several units as required. Then the new content of the activation field 79 is used by the controller 13 to calculate the new address of the next counter record 74, in this example the counter record 74c. The controller 13 saves the decremented value as the next counter value 76c the incremented content of the activation field 79 in the management field 75c, and calculates the new checksum based on the content of the counter value 76c and saves the new checksum in the field 77c.

If a power failure occurs, before the checksum is properly stored in the field 77c, the checksum is not correct. During the next access contact of the IC-card 2 (figure 1) with a card reader 1 (figure 1) the controller 13 addresses the counter record 74c and recalculates the checksum based on the content of the counter value 76c. Obviously the newly recalculated checksum differs now from the content of the checksum field 77c, because the previous transaction process failed at the arithmetic step 58 (figure 4), i.e. in the previous transaction the incrementing step 65 (figure 4) and the acknowledge step 69 (figure 4) have not been executed and the subtracted transaction amount has not been used for payment. If the checksum comparison fails, the controller 13 decrements therefore the content of the activation field 79 by one unit and reads out the counter value 76b, e.g. the previous cash value unit counter content 10' (figure 2), as the actual cash value unit counter content 10. The controller 13 proceeds as above, testing the checksum in the field 77b which is obviously correct, increasing the activation field 79 by one unit, decrementing the cash value unit counter content 10 according to the new transaction, and storing the new actual contents in the fields 75c, 76c, and 77c of the counter record 74c. This procedure has the advantage that the owner of the IC-card 2 can not fool the system by manually interrupting the process of transaction nor is it sensitive to accidental wrong handling or to a defective card reader 1 causing power failures in the IC-card 2.

If the checksum comparison fails more than two times in succession, the controller 13 decides that the respective counter record 74 contains defective memory cells and invalidates the IC -card 2 by setting the life cycle status LS to "Not Valid".

Once the secret keys are discovered, the system with preloaded IC-cards 2 of prior art has no provision to change the key in order to restore the security except to exchange all IC-cards 2 against a new series of IC-cards 2 as well as the associated security modules 4 causing the Issuer a loss of trust and a huge financial damage.

In Figure 2 the third E^2PROM memory section 19 provides a memory place 80 for an auxiliary key AK. The auxiliary key AK is not used for the standard processes. A value is filled in the memory place 80 and is used as the auxiliary key AK during the "Issuer Mode". The integrated circuit 8 deciphers a new cryptographic key K with the auxiliary key AK solely in case of a key downloading from the security module 4 (figure 1), e.g. after the cryptographic key K used in the algorithm circuit 29 was discovered. Obviously, the auxiliary key AK is also available in the security module 4. The advantage of this scheme is that the Issuer has only to initialise the key change procedure within the security modules 4 (figure 1) in an extra maintenance of the card readers 1 (figure 1) which is not obvious to the public. During the extra maintenance the new cryptographic key K is transferred to the security module 4 replacing the obsolete old key K* which is saved at another memory place within the security module 4. This also activates the key - change process. Thus there is no need to shut down the card operation during this extra maintenance of all card readers 1, because the key change process is already part of the authentication process but for clarity sake not shown in the figure 3.

Figure 8 shows the relevant part of the authentication process with the additional steps of the key - change process. The card signature is transferred to the security module 4 in the authentication request 41. If in the authentication test 42 using the new key K, the security module 4 classifies an IC-card 2 based on the card signature as not authentic, the IC-card 2 may use still the obsolete old key K* or be indeed not authentic. A switch 81 activated during the extra maintenance diverts the process to a second authentication test 42' where the card signature is recalculated using the obsolete old key K* and the result is compared with the transferred card signature. If the recalculated and the transferred card signatures differ, the IC-card 2 is not authentic and the process is diverted by a second switch 82 back to the terminal 3 with the security module status byte set to "Not Authentic". However, if the recalculated and the transferred card signatures are equal, the security module status

byte is set to "Change Key", and the second switch 82 diverts the process to a send key step 83. In the send key step 83 the new key K is encoded by the T-DES unit 11 (figure 1) using the DES - transformation with auxiliary key AK, the same as is stored at the memory place 80 (figure 2), and the transmitted card signature. The T-DES unit 11 prepares a message authentication code using the new key K and the transmitted card signature. The security module 4 then transmits the security module status byte, the encrypted new key and the message authentication code to the terminal 3. There the first decision 43 detects the security module status byte set to "Change Key", and the terminal 3 sends the encrypted new key and the message authentication code as a key change request to the IC-card 2. At the key verifying step 84 the algorithm circuit 29 (figure 2) decodes the encrypted key by the inverse DES - transformation using the auxiliary key AK stored at memory place 80. The result is the new key K which in turn is used to recalculate the message authentication code at a code step 85. The comparator 47 (figure 2) compares the recalculated message authentication code and the transmitted message authentication code. If both codes are the identical, i.e. if the comparator 47 senses "True", then the controller 13 (figure 2) considers the transmission of the encrypted key and the message authentication code as correct, replaces the old cryptographic key K by the new key K in the third E^2PROM memory section 19 (figure 2), sets the authenticate flag to "Access OK", and increments the faulty access number 48 by one unit. The process returns to the terminal 3 at the second decision 50. From then on the IC-card 2 will use the new key K instead of the original, but now obsolete key K*. However, if the result of the comparator 47 is "Not true", then the authenticate flag is set to "Access OK", the faulty access number 48 remains reduced by one unit, i.e.. the access is considered by the controller 13 as an invalid access attempt. Finally, the life cycle status byte is refreshed to "User Mode" and the process returns to the second decision 50 (figure 3).

If the increment and decrements act directly on the faulty access number 48 as described above, at logic status changes of the least significant bit of the faulty access number 48 is changed least four times. The limited life of an E^2PROM memory cell of about 100'000 cycles restricts the number of authentications to about 50'000. An alternative to the tracking of the number of invalid access attempts is now explained in detail.

In figure 9 two fields of the fourth E^2PROM memory section 20 are shown, the first field is called a Brute Force Attack ("BFA") counter 86 comprising the faulty access number 48 and the second field a ratification area 87 with an even number of bits 88. During a previous access of the IC-card 2 (figure 1), e.g. in the "Issuer Mode", the faulty access number 48 is set to an initial value representing the maximum number of allowed invalid attempts. At the same time the bits 88 of the ratification area 87 are set to logic one, e.g. if the ratification area 87 is 16 bits wide from the bit 88a to the bit 88q, the hexadecimal representation of the content of the ratification area 87 is "FFFF". Instead of subtracting one unit from the faulty access number 48 each time the authentication process is started, e.g. at the beginning of the encoding step 40 (figure 3) and of the arithmetic step 58 (figure 4) etc., the logic state of one of the 16 bits 88a to 88q is inverted by the controller 13 (figure 2) so that the number of bits 88 being in the same logic state (either zero or one) is an odd number (marking step). The parity of the number of bits 88 being in the same logic state (zero or one) is subsequently referred to as "bit parity". The bit parity is used as the content of the authenticate flag, e.g. a logic zero indicates an even parity and a logic one an odd parity. If the authentication fails, the terminal 3 (figure 1) aborts the process at the stops 44 (figure 3) or 60 (figure 4) and the controller 13 sets the invalidate line 30 (figure 2) to active and will not receive any further instruction from the second ROM 15. The IC-card 2 has to be reset by a signal on the reset line 24 (figure 2) in order to restart the authentication process again. On the other hand, if the authentication is correct, the controller 13 inverts the logic state of a neighbouring bit 88 in order to change the bit parity to even (regularizing step).

Returning now to the authentication process of the figure 3. After the reset of the IC-card 2 at reset step 32 the controller 13 (figure 2) tests in the preparation step 33 the faulty access number 48 (figure 2) at the card check 331. In case the faulty access number 48 exceeds zero, the authentication process enters first an additional bit parity check 335 within the random step 334 before the tasks of the random number step 334 are started. The bit parity check 335 determines the bit parity of the ratification area 87 (figure 9) and branches the process depending of the bit parity value. An even bit parity assures the controller 13 that any previous authentication was correct. If the bit parity is odd which indicates that the previous use of the IC-card 2 was irregular, the controller 13 changes the bit parity to even by inverting the logic

state of one of the 16 bits 88a (figure 9) to 88q (figure 9) in the ratification area 87 and decrements the faulty access number 48 by one unit. Then the authentication process exits the bit parity check 335 and proceeds with the tasks of the random step 334.

The advantage of the use of the ratification area 87 is that the faulty access number 48 is only decremented and that the change of the E^2PROM memory cells occurs only after an incorrect event (power failure etc.) which enhances the longevity of the E^2PROM memory cells involved.

At the beginning of the encoding step 40, the controller 13 changes the bit parity to odd by inverting the logic state of one of the 16 bits 88a to 88q in the ratification area 87 before the algorithm unit 29 (figure 2) calculates the card signature. In the execution of the IC-card 2 where the surveillance of the mutual authentication process is started already at the preparation step 33, the bit parity change may occur between the bit parity check 335 and the random number step 334, instead.

Also, at the beginning of the arithmetic step 58 (figure 4) the controller 13 changes the bit parity in the ratification area 87 to odd if the life cycle status LS is set to "User Mode" and the mutual authentication is assured.

At the end of the verifying step 46 (figure 3) and the arithmetic step 58 the controller 13 changes the bit parity in the ratification area 87 again to even, if the controller 13 senses that the mutual authentication was successful and the checksum is placed properly in the checksum field 77 (figure 6), respectively. Otherwise, if the controller 13 senses an unsuccessful authentication, the controller 13 keeps the bit parity in the ratification area 87 in the odd state. The authenticate flag carrying the bit parity information is then presented to the terminal 3 which branches the procedure at the second decision 50 to the stop 44 and at the third decision 59 to the stop 60, respectively, if the authenticate flag is set to a logic one. Such a failed access leaves an odd bit parity in the ratification area 87.

By virtue of inverting only one bit 88 in the ratification area 87 allows to increase the number of the authentications markedly, e.g. in the example of the 16 bit wide ratification area 87 the increase is 16 - fold to about 800'000 authentications without sacrificing the advantage of the E^2PROM memory cells, that the configuration of the

bits 88 in the ratification area 87 is lost during a powerless period until a next access to a card reader 1 (figure 1). Furthermore, in most access attempts more than one bit of the content of the faulty access number 48 has to be changed, which is a slow and energy consuming process with E^2PROM memory cells and is unacceptable during a normal authentication and payment transfer.

The change of the bit parity is now described in detail. The controller 13 reads the ratification area 87 and tests each of the bits 88 starting with the least significant bit 88a and going up to the most significant bit 88q. If the most significant bit 88q is a logic one, the controller 13 determines and marks the first bit starting from the bit 88a which contains a logic one. If the most significant bit 88q is a logic zero, the controller 13 determines and marks the first bit starting from the bit 88a which contains a logic zero. If this marked bit is one of the bits 88a, 88c, 88e, 88g, 88i, 88l, 88n and 88p, the controller 13 considers the bit parity in the ratification area 87 as even. In the case one of the other bits 88 is marked the bit parity is considered as odd. The bit parity in the ratification area 87 is stored in the authenticate flag. For each change of the bit parity the controller 13 inverts the logic state of the marked bit, only, i.e. the controller 13 converts a logic one into a logic zero or vice versa.

The advantage for the security of the information transfer is now clear. The life cycle status byte comprising the life cycle status LS and the authenticate flag are the only information to be sent in clear, however the information of the life cycle status byte does not allow any conclusions on the information contained in the IC-card 2. All other information exchanged is efficiently and securely scrambled.

In figure 10 an example of the life cycle status byte is shown located in the RAM memory section 16. The first E^2PROM memory section 17 comprises a memory space 89 of which seven bits 88 are used to save the life cycle status LS in the not volatile memory. The information at the memory space 89 is only changed to alter the life cycle status. For the refreshing of the life cycle status byte mentioned above a byte area 90 of the RAM memory section 16 is used. At the preparation step 33 (figure 3) and at each start of this refreshing process the controller 13 (figure 2) reads out the memory space 89 and copies its content into the byte area 90, e.g. into the seven least significant bits indicated by LS. Then the controller determines the state of the authentication flag and places a single bit flag 91 with the information about the

authentication flag at the most significant bit of the byte area 90. The life cycle status byte comprises therefore the life cycle status LS and the authenticate flag. The controller 13 always reads the life cycle status byte out of the byte area 90 and present it to the terminal 3 (figure 1).

The preloaded IC-card 2 (figure 2) of prior art have no means to identify themselves prior to customisation at the Issuers' premises. At the customisation step in the "Issuer Mode" the secret cryptographic keys together with the customisation data are copied into the preloaded IC-cards 2. There are no means to prevent the loading of the secret cryptographic keys in a look - alike IC-card 2 which imitates the real one. The look - alike IC-card 2 will accept the secret cryptographic keys and the customisation data and from there the secret cryptographic keys and the customisation data can be retrieved. The secret cryptographic keys are thus discovered and the security of the whole system is broken.

In figure 11 shows an integrity check at a terminal 3 dedicated for card customisation used at the Issuer's premises, only. The IC-card 2 is connected to the terminal 3 as well as a key bearer 92 on loan from a trusted third party to the Issuer. The key bearer 92 has an integrated circuit 92 of the identical design as the integrated circuit 8 of the IC-card 2 and comprises therefore the same functionality blocks bearing the same reference numbers but marked with a dash: an algorithm circuit 29', a ROM memory section 15' containing the operating system and at least a fourth E^2PROM memory section 20', etc. The key bearer 92 has for example the physical form of a normal IC-card 2 or the one of the security module 4 (figure 1) in order to fit the key bearer 92 into one of the socket 7 (figure 1) of the card reader 1. The ROM memory section 15' stores the identical operating program as the ROM memory section 15 and the fourth E^2PROM memory section 20' which may be empty is a copy of the fourth E^2PROM memory section 20 of the IC-card 2 to be personalised.

To start the customisation, the IC-card 2 is put into the card reader 1. The terminal 3 powers up the IC-card 2 in the reset step 32 (figure 3). The IC-card 2 starts to test the life cycle status LS according to the preparation step 33 (figure 3) and presents the refreshed life cycle status byte to the terminal 3. The terminal test 34 tests the life cycle status byte. If the life cycle status LS is set to the "Test Mode" the procedure is switched to an identifying step 94, otherwise the procedure is aborted at stop 36. In

the identifying step 94 the terminal 3 sends an identical challenge 95, e.g. the date and/or the actual time or a random number, to the IC-card 2 and to the key bearer 92. The challenge 95 may be send to the IC-card 2 and the key bearer 92 at the same time or at different times. The algorithm circuits 29 and 29' independently perform on their own the DES operation based on the challenge 95, and e.g. on the contents of the ROM memory section 15 and 15', and the fourth E^2PROM memory section 20 and 20', respectively. The results of both DES - operations are presented to the terminal 3. There the results of both DES - operations are presented to an identification decision 96 to be compared. If the two results are different then the procedure is aborted at the stop 97 because IC-card 2 is considered as defective or as a non-authentic simulator ("Trojan horse"). If the two results are equal then the terminal 3 starts the customisation 98 of the IC-card 2 and loads at least the relevant data and the secret key(s) taken from the key bearer 92, e.g. stored in a third E^2PROM memory section 19', via the terminal 3 into the third and fourth E^2PROM memory section 19 and 20, respectively. After verification of the transferred content the life cycle status LS stored at the memory space 89 (figure 10) is set by the controller 13 (figure 2) to "User Mode". The terminal 3 ends the customisation of the IC-card 2 as soon as the terminal 3 receives the refreshed life cycle status byte and senses the life cycle status LS = "User Mode" and the authenticate flag "Access OK".

The fourth E^2PROM memory section 20 has now a content different from the fourth E^2PROM memory section 20' which remains empty. Thus a second loading of these sensitive data into the IC-card 2 is impossible even if the IC-card 2 is removed from the card reader 1 before the life cycle status LS is set to "User Mode". The response of the IC-card 2 at the identification decision 96 differs from the one of the key bearer 92. The life cycle status LS of the personalised IC-cards is not anymore in the "Issuer Mode" the IC-card 2 will be rejected at the terminal check 34 and sent to stop 36. The advantage of this authentication prior to the customisation is the enhanced security against the discovery of the secret cryptographic keys and the "illegally refreshing" of used cards at the premises of the Issuer.

Claims

1. System comprising a card reader (1) with an electronic terminal (3) and at least one security module (4) and a portable preloaded IC-card (2) with an integrated circuit (8) having a lock (9) to prevent unauthorized use of the IC-card (2), and a non volatile memory section (20) to store a current IC-card value (10), with means to stepwise devaluate the current IC-card value during a transaction at a stand alone point of sale (56) connected to the terminal (3) of the card reader (1), and that the terminal (3) provides communication channels (5, 6; 7) between the IC-card (2) and the security module (4) characterized in that the IC-card (2) has means (9, 21, 28, 29) to generate a card random number and a card signature, and to present them to the security module (4), that the security module (4) has means (11, 12) to generate a security module random number and a security module signature, and to present them to the IC-card (2), that the IC-card (2) has a cryptographic key K and the means (29) for creating the card signature based on at least the security module random number and for decoding the security module signature to verify the authenticity of the security module (4), that the security module (4) has the cryptographic key K and the means (11) to create the security module signature from at least the card random number and to decode the card signature to verify the authenticity of the IC-card (2), that the integrated circuit (8) comprises a general purpose memory section (16) with an area (49) storing at least the card random number and the security module random number, and the lock (9) which is capable to allow the payment transaction to take place upon a positive mutual authentication of the IC-card (2) and the security module (4).

2. System according to claim 1 characterized in that the IC-card (2) and the security module (4) comprise an algorithm circuit (29) and a T-DES unit (11), respectively, for executing T-DES transformations with the cryptographic key K on data to be mutually exchanged and verified.

3. System according to one of the claims 1 or 2 characterized in that the security module (4) has means to replace an obsolete cryptographic key K* of the IC-card (2) by a new cryptographic key K, that an auxiliary key AK stored in a memory

place (80) of the IC-card (2), and that the auxiliary key AK is used solely for decoding the new cryptographic key K downloaded into the IC-card (2).

4. Preloaded IC-card (2) with an integrated circuit (8) having a lock (9) to prevent unauthorized use of the IC-card (2), non volatile data memory sections (17 to 20) to store at least an actual IC-card value (10), which is stepwise devaluated during a payment transaction, and communication channels (5, 21) to present data to the outside world, non volatile program memory sections (14 , 15), an area (80) of general purpose memory section (16), and a card random number generator circuit (28) generating a card random number, characterized in that said general purpose memory section (16) comprises means to temporarily store of at least the card random number, a card signature, a security module random number and a security module signature, said non volatile data memory sections (17; 18; 19; 20) comprise means to store at least a faulty access number (48), a cryptographic key K and the previous IC-card value (10'), said lock (9) comprises means to prevent the access to the card depending on the faulty access number (48), and it further comprises means to update the faulty access number (48) in case of invalid access attempt, an algorithm unit (29) using the cryptographic key K to encode the card signature and to decode the security module signature, and with a comparator (47) to verify the received security module signature.

5. IC-card (2) according to claim 4 characterized in that the non volatile data memory section (20) comprises a faulty access section (86) containing the faulty access number (48) and a ratification area (87) as an indicator of a previous access ending irregularly, and that the integrated circuit (8) is equipped with means (9, 13) to investigate the ratification area (87) and to update the faulty access number (48) in case the ratification area (87) indicates an irregular access.

6. IC-card (2) according to one of the claims 4 or 5, characterized in that the non volatile data memory sections comprise a backup counter area (74) dividing in at least two counter records (70), each record comprises counter values (76) representing either the actual IC-card value (10) or at least the previous IC-card value (10') and management data (75,77) indicating the order of transactions stored at the counter records (70), and that means are provided to update the

management data (75,77) of the actual IC-card value (10) and to use the previous IC-card value (10') for a payment transaction if the updated management data and the management data of the actual IC-card value (10) stored in the respective counters record (70) differ.

7. IC-card (2) according to one of the claims 4 to 6, characterized in that cells of the non volatile data memory section (17 to 20) are physically covered by a shield (27) and that the integrated circuit (8) has means (13) to erase sensitive data stored into the non volatile data memory sections (17 to 20) if any damage to the shield (27) is detected.

8. IC-card (2) according to one of the claims 4 to 7, characterized in that the non volatile data memory section (19) provides a memory place for an auxiliary key AK used to decode a new cryptographic key K and that the controller (13) is able to replace an obsolete key K* by the new one.

9. IC-card (2) according to one of the claims 4 to 8, characterized in that the non volatile data memory section(17) comprises an individual card number and that said individual card number is a parameter of the cryptographic calculations.

10. A method for mutual authentication between an IC-card (2) and a security module (4) located in a card reader (1) having a terminal (3) for a data exchange between the IC-card (2) and the security module (4) comprising the steps of :

- generating a card random number by the IC-card (2) and transferring it to the security module (4),

- generating a security module random number by the security module (4) and transferring it to the IC-card (2),

- calculating a card signature by the IC-card using at least a cryptographic key K and the security module random number, transferring it to the security module,

- calculating a card signature by the security module (4) using at least a cryptographic key K and the security module random number and comparing it to the transferred card signature, stopping the process if both signatures differ,

- calculating a security module signature by the security module (4) using at least a cryptographic key K, the card random number and the card signature and transferring it to the IC-card (2),

- calculating a security module signature by the IC-card (2) using at least a cryptographic key K, the card random number and the card signature and comparing it to the transferred security module signature, stopping the process if both signatures differ.

11. A method according to claim 10 characterized in that the card random number is transferred from the IC-card together with at least a unique serial number of the IC-card, the cryptographic key K being determined by the security module using the unique serial number.

12. A method according to claims 10 and 11 characterized in that, it further comprises the step of updating a faulty access number (48) in case of unsuccessful comparison.

13. A method according to claim 12 characterized in that, prior to start the mutual authentication process, the IC-card (2) check the content of the faulty access number (48) representing the number of invalid access attempts and disable the access of the IC-card (2) in case the faulty access number (48) has reached a predetermined limit.

14. A method according to claims 10 to 13 characterized in that, it further comprises the steps of marking by the IC-card a ratification area in the non volatile data memory section when transferring the first card signature, and regularizing the ratification area after a successful signatures comparison.

15. A method according to claim 14 characterized in that, updating the ratification area comprises the following steps:

- executing, after the card check (331) and before generating the card random number, a check on the bits (88) stored in the ratification area (87),

- updating the faulty access number (48) and regularizing the bits (88) of the ratification area (87) in case that the ratification area indicates an unterminated session,

- marking the bits (88) in the ratification area (87) to indicate the start of the session,

- regularizing the bits (88) in the ratification area (87) in case of successful terminated session.

16. A method according to claim 15 characterized in that, marking or regularizing the bits (88) in the ratification area (87) is made by inverting a single bit after the other.

17. A method according to one of the claims 10 to 16 characterized in that a payment transaction, comprises at least the steps of

- calculating by the security module (4) a cryptogram based on at least the previously exchanged cryptogram and the amount to be decreased, transferring it to the IC-card (2) with the amount to be decreased,

- calculating by the IC-card (2) a cryptogram based on at least the previously exchanged cryptogram and the amount to be decreased, comparing it with the received cryptogram and decreasing internal counter if both cryptograms are equal,

- calculating by the IC-card (2) a cryptogram based on at least the previously exchanged cryptogram and the current IC-card value, transferring it to the security module (4),

- calculating by the security module (4) a cryptogram based on at least the previously exchanged cryptogram and the expected current IC-card value, comparing it with the received cryptogram, and successfully terminate the transaction and updating the IC-card value if both cryptograms are equal.

18. A method according to claim 17 characterized in that, updating the IC-card value comprises the following steps:

- addressing a next counter value record, each record comprises at least a counter value (76) representing either the actual IC-card value (10) or the previous IC-card value (10') and management data (75,77),

- storing the current IC-card value in the addressed counter value record,

- updating and storing its corresponding management data in the addressed counter value record.

19. A method according to claim 10 to 18 characterized in that in case the security module (4) recognizes that the IC-card (2) is still using an obsolete cryptographic key K*, the following steps of a key change process are executed :

- sending by the security module (4) an encrypted new key K using an auxiliary key AK to the IC-card (2) and an authentication cryptogram (MAC) which is at least based on the new key K or the encrypted new key K and the previously transferred card signature,

- decoding by the IC-card (2) the encrypted new key K using the auxiliary key AK,

- calculating an authentication cryptogram (MAC) which is at least based on the new key K or the encrypted new key K and the previously transferred card signature,

- comparing the transferred and the calculated authentication cryptograms, and if both are identical,

- replacing the current key K* with the new key K.

Fig. 1:

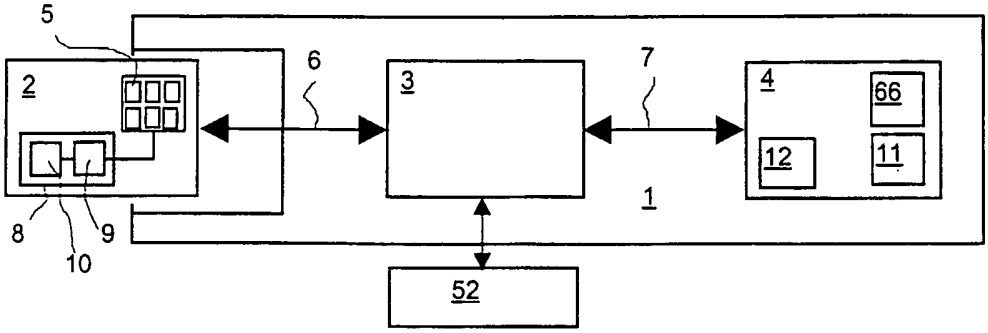

5
2
6
3
7
4
66
12
11
1
8
9
10
52

Fig. 2:

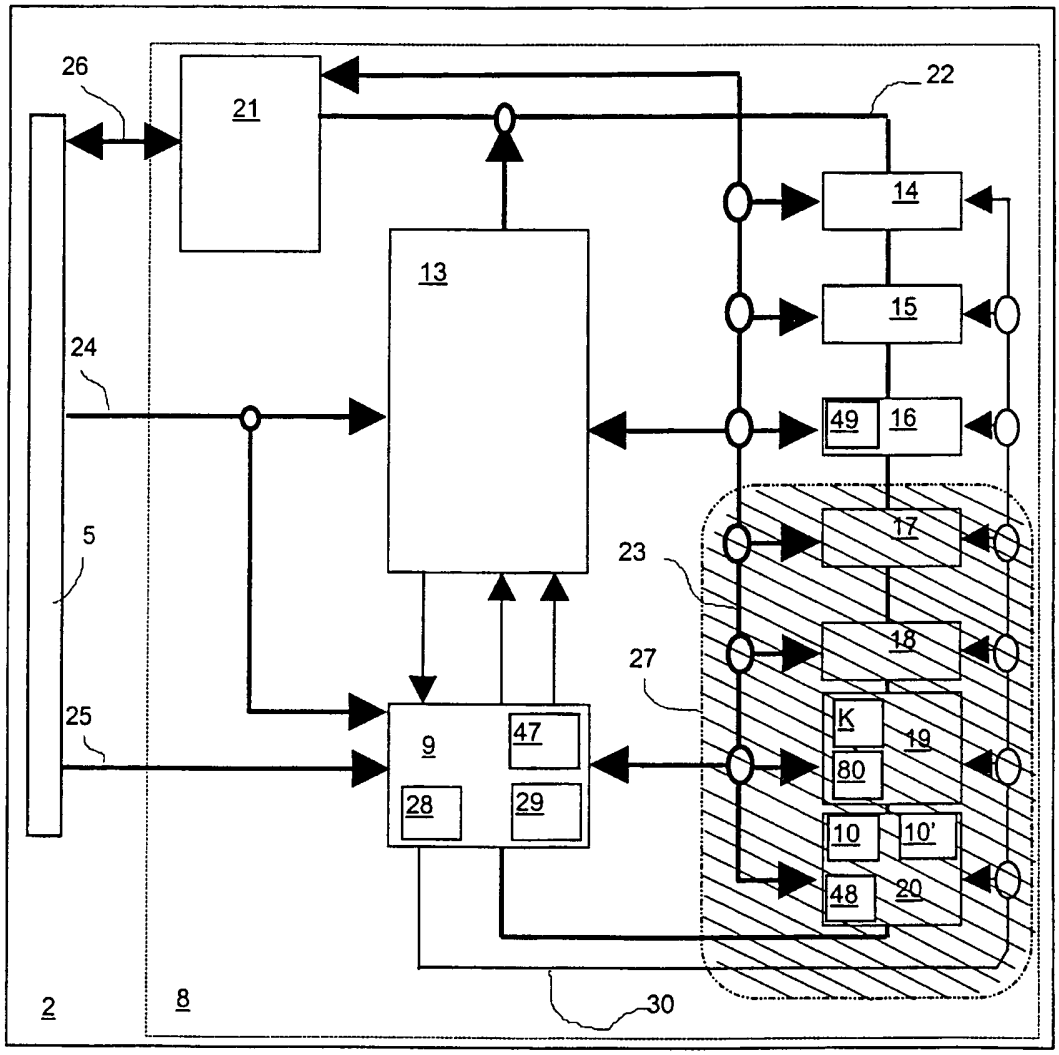

26
21
22
14
13
15
24
49
16
17
5
23
18
27
K
19
25
9
47
80
28
29
10
10'
48
20
2
8
30

Fig. 3:

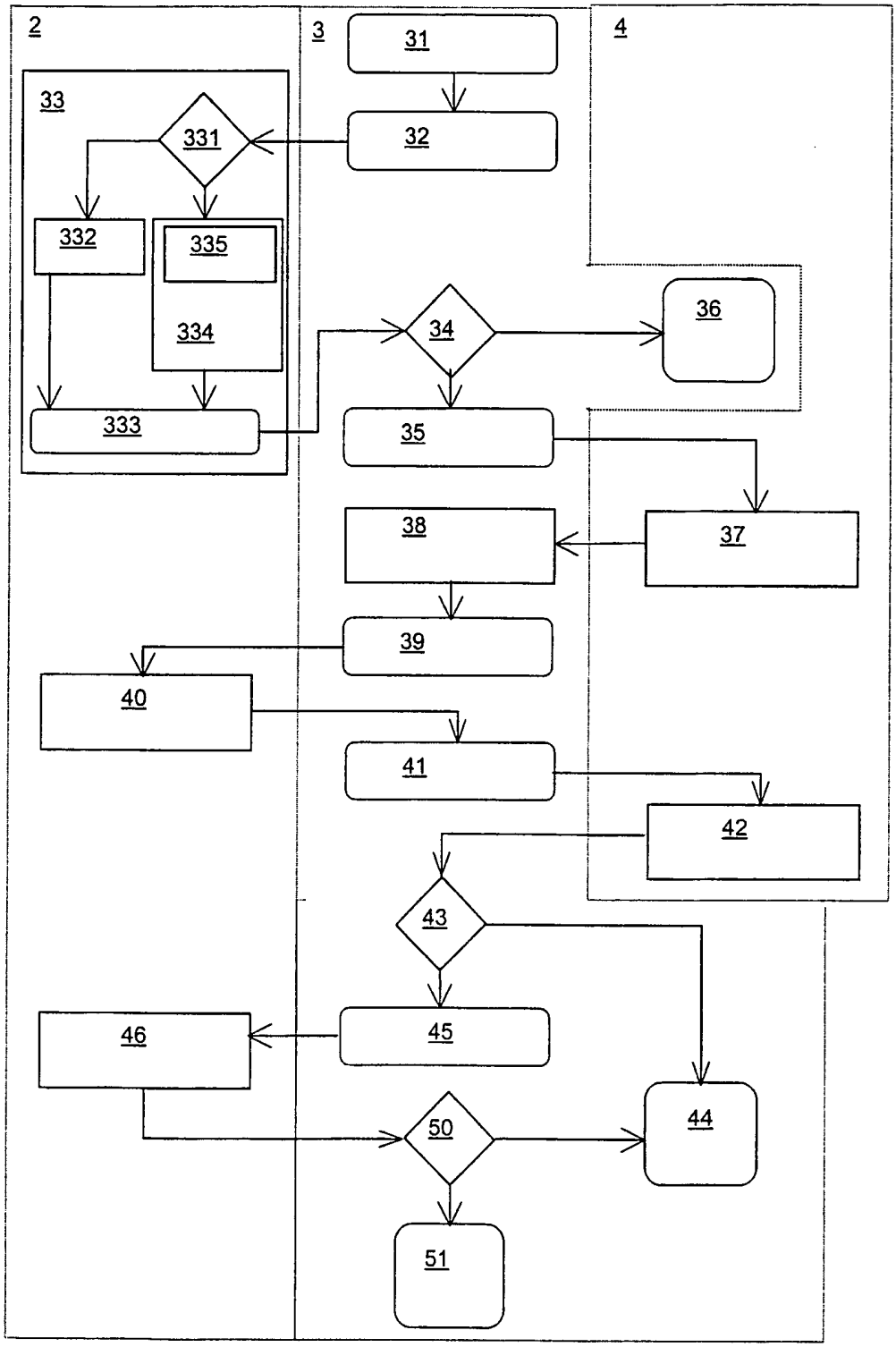

2
3
4
31
32
33
331
332
335
334
333
34
36
35
38
37
39
40
41
42
43
46
45
44
50
51

Fig. 4:

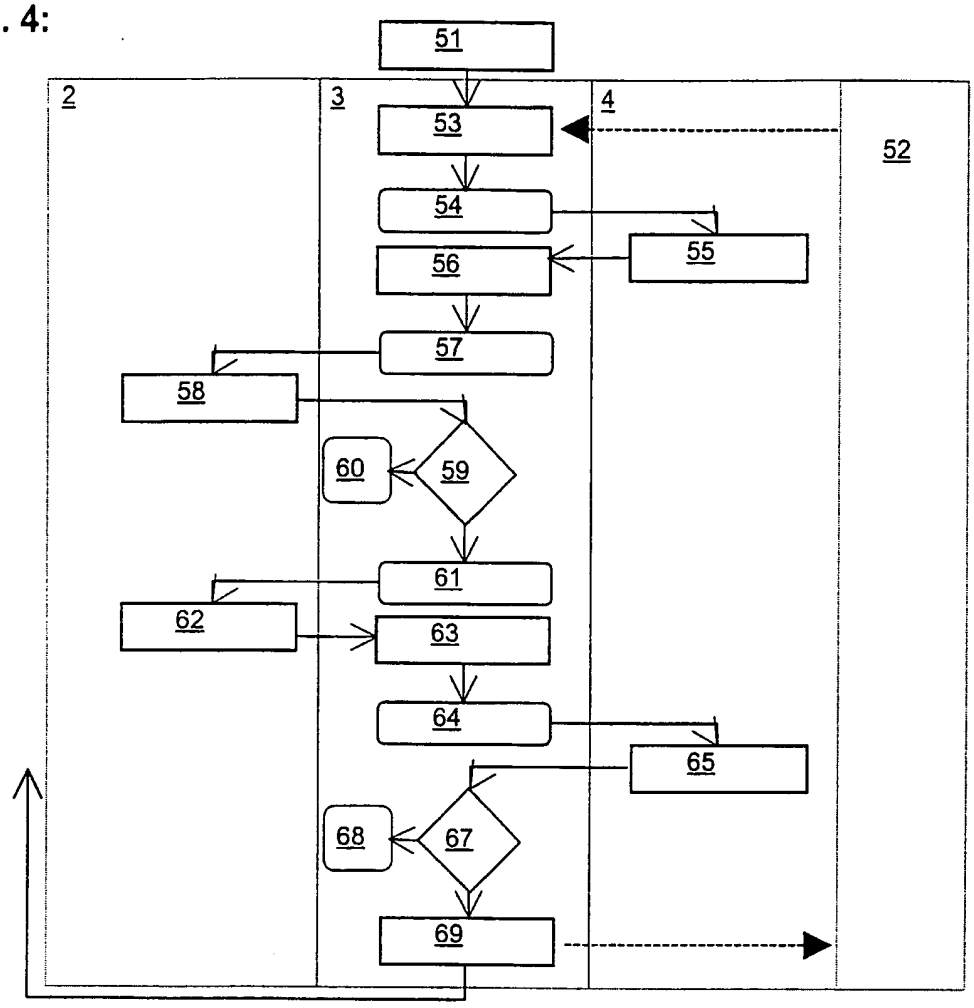


Fig. 5:

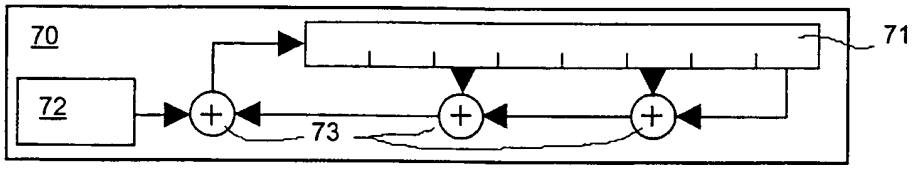


Fig. 6:

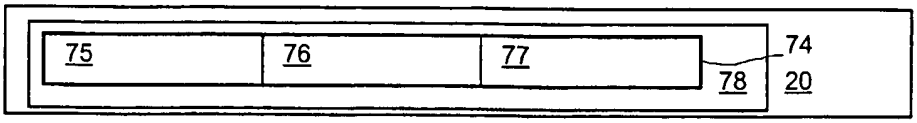


Fig. 7:

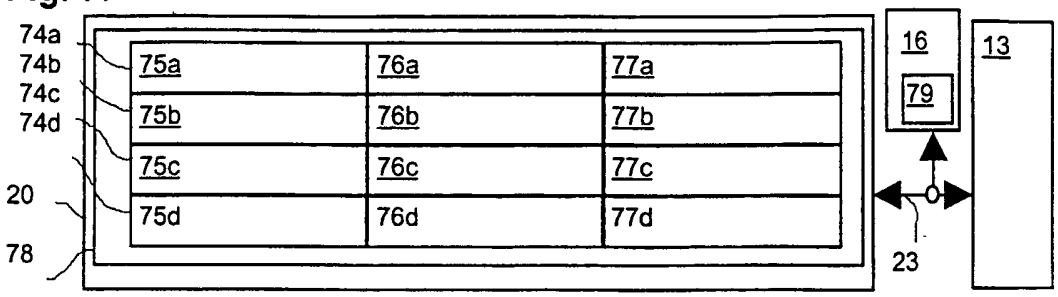


Fig. 8:

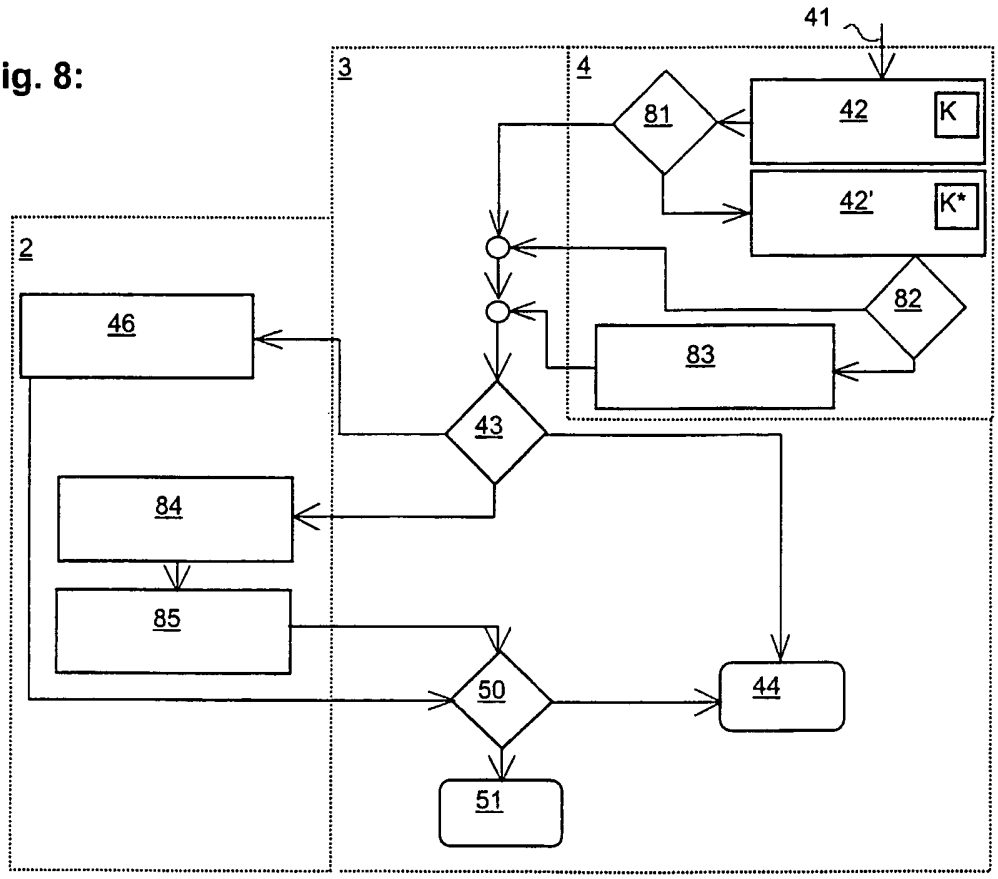


Fig. 9:

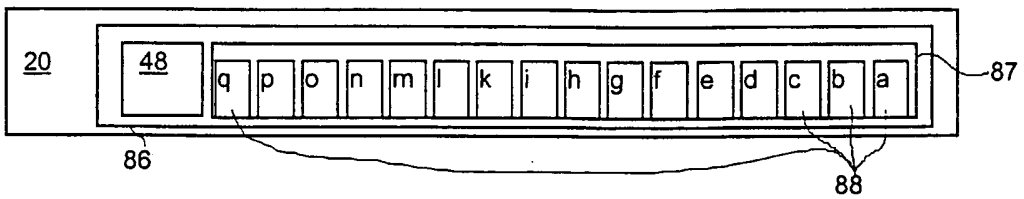


Fig. 10:

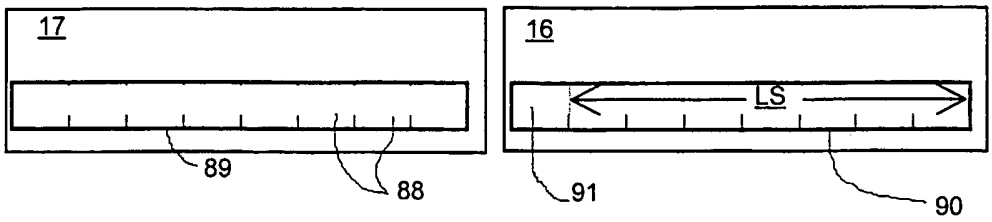
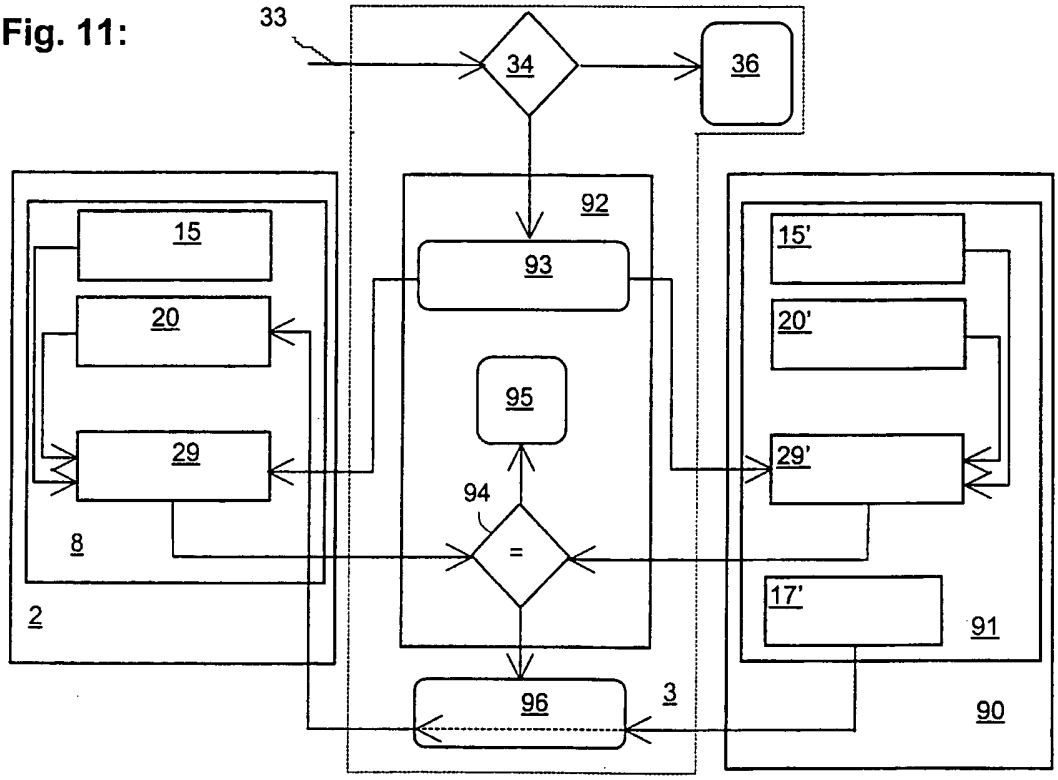

17
16
LS
89
88
91
90

Fig. 11:


33
34
36
92
15
93
15'
20
20'
95
29
29'
94
=
8
2
17'
91
96
3
90

INTERNATIONAL SEARCH REPORT

Intern ıal Application No
PCT/IB 99/00977

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 817 420 A (SONY CORP) 7 January 1998 (1998-01-07) abstract; figures 1,2,6-9 column 5, line 25 - column 6, line 18 column 7, line 27 - column 11, line 41	1
Y		2

X	EP 0 727 894 A (KOKUSAI DENSHIN DENWA CO LTD) 21 August 1996 (1996-08-21) abstract; figure 9 column 16, line 29 - column 17, line 48	1
A		4,9-11

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 August 1999	22/09/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Buron, E

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interr ıal Application No
PCT/ıB 99/00977

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X,P	EP 0 856 820 A (TOKYO SHIBAURA ELECTRIC CO) 5 August 1998 (1998-08-05) abstract; figures 1,3,9 column 1, line 28 - column 2, line 53 column 4, line 13 - line 51 column 6, line 38 - column 7, line 36	1
Y	O'MAHONY, PIERCE, TEWARI: "Electronic Payment Systems" , ARTECH HOUSE, INC. , 1997 XP002113876 page 25, paragraph 3.2.2	2
Y	DE 44 42 357 A (DEUTSCHE TELEKOM AG) 5 June 1996 (1996-06-05) abstract; figures column 2, line 49 - column 4, line 31	4
A		1,10
Y	EP 0 789 335 A (DEUTSCHE TELEKOM AG) 13 August 1997 (1997-08-13) abstract; figure column 3, line 1 - line 58	4
A		9
A	DE 195 06 921 A (ORGA KARTENSYSTEME GMBH) 29 August 1996 (1996-08-29) abstract; figure 2 column 2, line 40 - line 61	5,12-16
A	WO 93 20538 A (TELSTRA CORP LTD ;ZUK EDWARD ANDREW (AU)) 14 October 1993 (1993-10-14) abstract; figure page 3, line 14 - page 9, line 11	3,8,19
A	FR 2 681 165 A (GEMPLUS CARD INT) 12 March 1993 (1993-03-12) abstract; figures page 1, line 24 - page 5, line 30	3,8,19
A	EP 0 398 545 A (DELCO ELECTRONICS CORP) 22 November 1990 (1990-11-22) abstract; figure 1 column 2, line 8 - line 38 column 3, line 1 - column 5, line 8	6
A	FR 2 580 834 A (GRANDMOUGIN MICHEL) 24 October 1986 (1986-10-24) cited in the application abstract; figure 1 page 1, line 2 - page 5, line 15	7

-/--

1

INTERNATIONAL SEARCH REPORT

Intern ıal Application No
PCT/ıB 99/00977

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 602 918 A (CHEN JAMES F ET AL) 11 February 1997 (1997-02-11) abstract; figure 3 column 3, line 44 - column 5, line 56	10

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intern ·al Application No
PCT/ıB 99/00977

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0817420 A	07-01-1998	JP 10020780 A	23-01-1998
		CN 1180865 A	06-05-1998
EP 0727894 A	21-08-1996	US 5761309 A	02-06-1998
		WO 9607256 A	07-03-1996
EP 0856820 A	05-08-1998	JP 10222618 A	21-08-1998
DE 4442357 A	05-06-1996	NONE	
EP 0789335 A	13-08-1997	DE 19604349 A	14-08-1997
DE 19506921 A	29-08-1996	DE 19548903 A	29-08-1996
WO 9320538 A	14-10-1993	AU 671986 B	19-09-1996
		AU 3818093 A	08-11-1993
		CA 2133200 A,C	14-10-1993
		EP 0634038 A	18-01-1995
		JP 7505270 T	08-06-1995
		SG 46692 A	20-02-1998
		US 5745571 A	28-04-1998
FR 2681165 A	12-03-1993	NONE	
EP 0398545 A	22-11-1990	JP 3019053 A	28-01-1991
FR 2580834 A	24-10-1986	NONE	
US 5602918 A	11-02-1997	CA 2241052 A	03-07-1997
		EP 0870382 A	14-10-1998
		WO 9723972 A	03-07-1997